PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
WPP290155		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/GB2005/000231	24/01/2005	25/03/2004
Applicant		
CRYPTOMATHIC A/S		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 7 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
      ☐ The international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).
   b. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (See Box II).

3. ☒ **Unity of invention is lacking** (see Box III).

4. With regard to the **title,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 3
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB2005/000231

CLASSIFICATION OF SUBJECT MATTER
G07C13/00 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G07C H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2003/178484 A1 (VADURA DENNIS ET AL) 25 September 2003 (2003-09-25) paragraph [0012] paragraph [0016] paragraph [0019] - paragraph [0020] paragraph [0043] paragraph [0052] - paragraph [0054] paragraph [0060] - paragraph [0061] -----	1-8, 13-17,22 9-12,20, 21,23-27
Y	"REPORT ON REVIEW OF CRYPTOGRAPHIC PROTOCOLS AND SECURITY TECHNIQUES FOR ELECTRONIC VOTING" CYBERVOTE, 28 January 2002 (2002-01-28), XP001176600 page 16 - page 18 page 22 - page 27 -----	9-12, 23-27

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 December 2005	27. 02. 2006

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Stenger, M

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB2005/000231

ontinuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/084325 A1 (REARDON DAVID C) 4 July 2002 (2002-07-04) paragraph [0008] paragraph [0016] paragraph [0019] paragraph [0022] paragraph [0027] paragraph [0032] - paragraph [0034]	1-8, 13-17,22
X	US 4 981 259 A (AHMANN ET AL) 1 January 1991 (1991-01-01) column 1, line 56 - column 2, line 13 column 2, line 52 - column 3, line 2	18,19
X	PATENT ABSTRACTS OF JAPAN vol. 018, no. 353 (P-1764), 4 July 1994 (1994-07-04) & JP 06 089296 A (SEIJI KOUHOU CENTER:KK; others: 01), 29 March 1994 (1994-03-29) abstract figures 3,16	18,19
Y	PATENT ABSTRACTS OF JAPAN vol. 002, no. 079 (E-040), 23 June 1978 (1978-06-23) & JP 53 044142 A (HITACHI LTD), 20 April 1978 (1978-04-20) abstract	20,21
A	PATENT ABSTRACTS OF JAPAN vol. 1997, no. 05, 30 May 1997 (1997-05-30) & JP 09 011677 A (NEC ENG LTD), 14 January 1997 (1997-01-14) abstract	20,21

INTERNATIONAL SEARCH REPORT

International application No.
PCT/GB2005/000231

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of Invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-27

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-17, 22-27

Problem to be solved:
To provide for an electronic voting system which provides security and integrity (p.5, last paragraph).
Solution:
Provide both an electronic ballot and a paper ballot which are linked by linking information and compare a sample of them according to independent claims 1, 15 and 22.

1.1. claims: 18,19

Problem to be solved:
To provide for a ballot box with the possibility of distributing ballots to two ballot holders.
Solution:
To provide a selector that selects substantially at random one of the two ballot holders according to independent claim 18.

1.2. claims: 20,21

Problem to be solved:
To be able to scan a specific information on a paper ballot without revealing another information on the same paper ballot.
Solution:
To configure the ballot such that both informations are visible, but not at the same time according to independent claim 20.

---

2. claim: 28

Problem to be solved:
To find a committment method (p.25, 3rd paragraph).
Solution:
Determine a commitment value from an electronic data value according to independent claim 28.

---

3. claims: 29-30

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Problem to be solved:
To find a method of providing information for verifying correctness of a permutation of encrypted messages.
Solution:
Sending commitments and additional information to a verifier according to independent claim 29.

---

4. claims: 31-32

Problem to be solved:
To find a method of providing information for verifying correctness of a combined permutation and partial decryption of encrypted messages.
Solution:
Sending information to a verifier such that the verifier can use a zero-knowledge protocol according to independent claim 31.

---

5. claims: 33-35

Problem to be solved:
To find a method for shuffling and decrypting encrypted electronic data by a plurality of data processing entities.
Solution:
Partially decrypting and re-randomising the electronic data using a secret key shares according to independent claim 33.

---

6. claims: 36-43

Problem to be solved:
To find a method of providing data for verifying that messages are authentic.
Solution:
Selecting random numbers and determining thereform verification values according to independent claims 36 and 37.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB2005/000231

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003178484 A1	25-09-2003	US 2003006282 A1	09-01-2003
US 2002084325 A1	04-07-2002	US 2006000906 A1	05-01-2006
US 4981259 A	01-01-1991	NONE	
JP 06089296 A	29-03-1994	NONE	
JP 53044142 A	20-04-1978	NONE	
JP 09011677 A	14-01-1997	JP 3295832 B2	24-06-2002